2131
#4

Attorney Docket No. 50325-0549

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

David McGrew

Serial No.: 09/982,375

Filed on: October 17, 2001

Group Art Unit No.: 2131

Examiner: NYA

For: ENCRYPTION METHOD AND APPARATUS WITH FORWARD SECRECY AND RANDOM-ACCESS KEY UPDATING METHOD

Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 together with copies of the documents cited on that form. It is respectfully requested that the cited documents be considered and that the enclosed Information Disclosure Citation Form PTO-1449 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

__X__ 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then this Information Disclosure Statement includes one of the following:

_____ A statement pursuant to 37 C.F.R. §1.97(e)

_____ 1.97(e)(1) The undersigned hereby states that each item of information contained in this information disclosure statement was first cited in communication from a foreign patent office in a counterpart

foreign application not more than three months prior to the filing of this information disclosure statement.

_____ 1.97(e)(2) The undersigned hereby states that no item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in this information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement.

_____ A check for $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then this Information Disclosure Statement includes the following:

_____ A statement pursuant to 37 C.F.R. §1.97(e)

_____ 1.97(e)(1) The undersigned hereby states that each item of information contained in this information disclosure statement was first cited in communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement; OR

_____ 1.97(e)(2) The undersigned hereby states that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement.

AND

_____ A check for $180.00 for the fee under 37 C.F.R. §1.17(i) for submission of the Information Disclosure Statement.

_____ 37 C.F.R. §1.97(i). Wherein applicants are submitting references before the grant of a patent to be placed in the file but not considered by the Patent office.

(1) Accordingly, copies of the references as listed on the attached Form PTO 1449 are submitted herewith for placement in the file. No certification or fees are deemed necessary.

Throughout the pendency of this application, please charge any additional fees, including any required extension of time fees, and credit all overpayments to deposit account 50-1302. A duplicate of this sheet is enclosed.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: February 20, 2002

Christopher J. Palermo
Reg. No. 42,056

1600 Willow Street
San Jose, California 95125-5106
Telephone: (408) 414-1080
Facsimile: (408) 414-1076

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, Washington, D. C. 20231 on February 20, 2002
(Date of Deposit)

Jennifer Newell
(Typed or printed name of person mailing correspondence)

(Signature of person mailing correspondence)

INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(PTO-1449)

ATTY. DOCKET NO.	SERIAL NO.
50325-0549	09/982,375

APPLICANT	
David McGrew	
FILING DATE	GROUP
October 17, 2001	2131

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE
	5,454,039	9/26/95	Coppersmith et al.	380	28	12/6/93
	5,675,652	10/7/97	Coppersmith et al.	380	28	6/7/95
	5,835,597	11/10/98	Coppersmith et al.	380	28	3/31/97

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," 2nd ed. (New York: John Wiley & Sons, 1996), pp. 400-402
	Rogaway, P. and Coppersmith, D., "A Software-Optimized Encryption Algorithm", Proc. of 1994 Fast Software Encryption Workshop, Lecture Notes In Computer Science, Vol. 809, Springer-Verlag, 1994, pp. 56-63, *reprinted in* J. Cryptology 11:4, Springer-Verlag, 1998, pp. 273-287, *and* http://www.cs.ucdavis.edu/~rogaway/papers/seal-abstract.html.
	M. Bellare et al., "Forward Integrity for Secure Audit Logs," Dept. Comp. Sci. Eng., Univ. Calif. at San Diego, Nov. 23, 1997.
	B. Schneier et al., "Cryptographic Support for Secure Logs on Untrusted Machines," Proc. Seventh USENIX Security Symposium, USENIX Press, Jan. 1998, pp. 53-62.
	S. Kent et al., "Security Architecture for the Internet Protocol," IETF Request for Comments (RFC) 2401, The Internet Society, Nov. 1998.
	S. Kent et al., "IP Authentication Header," IETF Request for Comments (RFC) 2402, The Internet Society, Nov. 1998.
	S. Kent et al., "IP Encapsulating Security Payload (ESP)," IETF Request for Comments (RFC) 2406, The Internet Society, Nov. 1998.
	D. Harkins et al., "The Internet Key Exchange (IKE)," RFC 2409, The Internet Society, Nov. 1998
	H. Orman, "The OAKLEY Key Determination Protocol," RFC 2412, The Internet Society, Nov. 1998.

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.